

ABSTRACT OF THE DISCLOSURE

A method for inserting a digital signature into digital data is provided. The digital data has bits and the method includes the steps of: assigning predetermined bits of the digital data for receiving the digital signature; signing the digital data excluding the predetermined bits resulting in the digital signature; and inserting the digital signature into the predetermined bits of the digital data for subsequent authentication of the digital data. Also provided is a method for authenticating digital data having the embedded digital signature in the predetermined bits of the digital data including the steps of: extracting the digital signature from the predetermined bits; decrypting the digital signature from the digital data resulting in a first hash; applying a known one-way hashing function used by an encoder of the digital data to the digital data excluding the predetermined bits resulting in a second hash; and comparing the first hash to the second hash wherein if the first hash matches the second hash the digital data is authentic. In a preferred version of the methods of the present invention, the method further includes the step of inserting associated data into the digital data prior to the signing step such that the digital signature authenticates both the associated data as well as the digital data. Preferably, the associated data is inserted into the bits of the digital data excluding the predetermined bits.